Forslag

til

Lov om den statslige varslingstjeneste for internettruslers behandling af personoplysninger

§ 1. Loven regulerer den under Ministeriet for Videnskab, Teknologi og Udvikling etablerede statslige varslingstjeneste for internettruslers behandling af personoplysninger indeholdt i pakke- og trafikdata.

Stk. 2. Kommuner, regioner og private virksomheder, der er beskæftiget med kritisk infrastruktur, kan anmode om tilslutning til den statslige varslingstjeneste for internettrusler.

Stk. 3. Ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler for de i stk. 2 anførte myndigheders og private virksomheders tilslutning til den statslige varslingstjeneste for internettrusler, herunder regler om betaling.

§ 2. I denne lov forstås ved:

1) Pakkedata: Indholdet af internetbaseret kommunikation.
2) Trafikdata: Data, som behandles med henblik på overføring af pakkedata, jf. nr. 1.
3) Sikkerhedshændelse: Hændelse, der påvirker tilgængelighed, integritet eller fortrolighed af information eller tjenester på internettet.

§ 3. Den statslige varslingstjeneste for internettrusler behandler, herunder registrerer, analyserer og opbevarer, uden retskendelse tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Den statslige varslingstjeneste for internettrusler må alene analysere indsamlede pakkedata i tilfælde af begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse og kun i det omfang, det er nødvendigt for den pågældende analyse.

Stk. 2. Den statslige varslingstjeneste for internettrusler sletter de i stk. 1 nævnte pakke- og trafikdata, når formålet med behandlingen er opfyldt. Uanset, at formålet med behandlingen ikke er opfyldt, kan

1) pakke- og trafikdata, der knytter sig til en konkret sikkerhedshændelse, maksimalt opbevares i tre år.

2) pakkedata, der ikke knytter sig til en konkret sikkerhedshændelse, maksimalt opbevares i 14 dage.
3) trafikdata, der ikke knytter sig til en konkret sikkerhedshændelse, maksimalt opbevares i 12 måneder.

Fristerne i nr. 1-3 beregnes fra tidspunktet for registreringen af de pågældende data i den statslige varslingstjeneste.

Stk. 3. Ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler for den i stk. 1 nævnte behandling af pakke- og trafikdata.

§ 4. Bestemmelserne om indsigelse i § 35 i lov om behandling af personoplysninger finder ikke anvendelse på den statslige varslingstjeneste for internettruslers behandling af personoplysninger.

Stk. 2. Personer, der virker inden for den statslige varslingstjeneste for internettrusler, har tavshedspligt, jf. borgerlig straffelov § 152, jf. § 152 a-e, med hensyn til oplysninger, som de gennem deres virksomhed i varslingstjenesten får kendskab til, jf. dog § 5.

§ 5. Den statslige varslingstjeneste kan kun videregive data, der er indsamlet som led i varslingstjenestens aktiviteter, i følgende tilfælde:

1) Pakkedata og trafikdata, der knytter sig til en konkret sikkerhedshændelse, kan videregives til politiet.
2) Trafikdata kan videregives til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande i henhold til varslingstjenestens formål.

§ 6. Ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, der følger den statslige varslingstjeneste for internettruslers virksomhed.

Stk. 2. Tilsynet består af en dommer som formand og fire sagkyndige medlemmer, Formanden og medlemmerne af tilsynet beskikkes af ministeren for videnskab, teknologi og udvikling. Ministeren for videnskab, teknologi og udvikling skal ved beskikkelsen af tilsynets medlemmer lægge vægt på, at tilsynet samlet repræsenterer juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab.

Stk. 3. Medlemmerne beskikkes for fire år ad gangen og kan genbeskikkes.

Stk. 4. Ministeren for videnskab, teknologi og udvikling fastsætter rammerne for tilsynets virksomhed. Ministeren for videnskab, teknologi og udvikling kan herunder beslutte, at tilsynet skal udarbejde en årsberetning om den statslige varslingstjeneste for internettruslers virksomhed.

Stk. 5. IT- og Telestyrelsen stiller sekretariatsbistand til rådighed for tilsynet.

Stk. 6. Staten afholder alle udgifter i forbindelse med tilsynets virksomhed.

§ 7. Ministeren for videnskab, teknologi og udvikling kan bemyndige en under ministeriet oprettet statslig myndighed eller efter forhandling med vedkommende minister andre statslige myndigheder til at udøve de beføjelser, der i denne lov er tillagt ministeren for videnskab, teknologi og udvikling.

Stk. 2. Ministeren for videnskab, teknologi og udvikling kan fastsætte regler om adgangen til at påklage afgørelser, der er truffet i henhold til bemyndigelse efter stk. 1, herunder om, at afgørelserne ikke skal kunne påklages.

Stk. 3. Ministeren for videnskab, teknologi og udvikling kan fastsætte regler om udøvelsen af de beføjelser, som en anden statslig myndighed efter forhandling med vedkommende minister bliver bemyndiget til at udøve efter stk. 1.

§ 8. Loven træder i kraft den 1. juli 2011.

§ 9. Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

5. De økonomiske og administrative konsekvenser for erhvervslivet
6. De administrative konsekvenser for borgerne
7. De miljømæssige konsekvenser
8. Forholdet til EU-retten
9. De hørte myndigheder og organisationer
10. Sammenfattende skema

1. BAGGRUND FOR LOVFORSLAGET

1.1. Indledning

1.1.1. Internettet og informationssystemer er blevet en afgørende faktor for den økonomiske og samfundsmæssige udvikling. Internettets og informationssystemernes sikkerhed og fleksibilitet får stadig større betydning for samfundet.

Det er regeringens vision, at Danmark skal være blandt verdens førende højteknologiske samfund. Det kræver, at borgere, virksomheder og det offentlige har adgang til avanceret infrastruktur for informations- og kommunikationsteknologi (ikt) og til effektivt at udnytte de muligheder, der følger med digitaliseringen. Det kræver også, at borgere og virksomheder er trygge ved ikt-anvendelsen og har tillid til tjenester på internettet.

Internettet er blevet en del af den kritiske infrastruktur. En række af de funktioner, som udføres af det offentlige, og som er væsentlige for statens virke, afhænger af internettet.

Det er nødvendigt at sikre, at systemernes sikkerhedsniveau er tilstrækkeligt til at sikre en fortsat og korrekt drift af de offentlige it-systemer. Den teknologiske udvikling gør det muligt at iværksætte omfattende elektroniske angreb på den internetbaserede infrastruktur, hvilket kan medføre sammenbrud. Sådanne sammenbrud kan få alvorlige konsekvenser for vitale samfundsfunktioner, uanset om de er forårsaget af hændelige uheld eller af bevidste handlinger.

Det er en kendsgerning, at angrebene på internettet bliver stadig mere sofistikerede, og at hackere stadig bliver hurtigere til at udnytte de sårbarheder, der løbende opstår i internettets komponenter.

Som eksempler på angreb mod nationale digitale infrastrukturer kan nævnes sikkerhedshændelserne i henholdsvis Estland i april 2007 og Georgien i august 2008. I begge tilfælde bestod angrebene af meget store mængder internettrafik (pakke- og

trafikdata) mod vigtige offentlige og private hjemmesider og systemer med den effekt, at de ikke længere kunne tilgås, ligesom sikkerhedshuller på hjemmesider blev udnyttet til at udskifte indholdet af disse. Angrebene var primært rettet mod tv-stationer, aviser, ministerier og politiske organisationers hjemmesider og medførte i både Estland og Georgien, at regeringerne fik svækket deres interne kommunikationskanaler samt muligheden for at kommunikere med befolkningen. Angrebene var således rettet mod både statens sikkerhed og pressefriheden.

I Estland blev angreb også rettet mod finansinstitutioners hjemmesider med en række alvorlige følger for finanssektoren. En større del af befolkningen kunne således ikke via internettet hæve penge eller udføre finansielle transaktioner i flere dage. Kreditkortterminaler, som kommunikerer med bankerne via internettet, blev også ramt.

Disse eksempler understreger, at et moderne samfund er afhængigt af et robust internet.

Behovet berøres i EU-Kommissionens meddelelse "Beskyttelse mod storstilede cyberangreb og sammenbrud: øget beredskab, sikkerhed og robusthed" af 30. marts 2009. Meddelelsen bygger videre på EU's ambition om at styrke sikkerhed i og tilliden til informationssamfundet. Kommissionen fremhæver i meddelelsen særligt strategien for et sikkert informationssamfund fra 2006.

I meddelelsen lægger Kommissionen vægt på forebyggelse, beredskab og bevidstgørelse og opstiller en plan over øjeblikkelige tiltag, der skal styrke sikkerheden og robustheden i kritisk informationsinfrastruktur. Et af disse tiltag er etablering af velfungerende statslige varslingstjenester i alle medlemslande inden udgangen af 2011.

I erkendelse af internettets vitale betydning besluttede regeringen i maj 2009 at oprette en statslig varslingstjeneste for sikkerhedshændelser på internettet, en såkaldt GovCERT (Government Computer Emergency Response Team).

Offentlige myndigheder kommunikerer i dag i høj grad via internettet med borgere og virksomheder. Med oprettelsen af GovCERT ønsker regeringen bl.a. at mindske risikoen for, at en eller flere offentlige myndigheders elektroniske kommunikation med omverdenen bliver afskåret i flere dage. Dette kan udgøre en sikkerhedsrisiko og også have store administrative og økonomiske konsekvenser til følge. Tilsvarende gør sig gældende for private virksomheder beskæftiget med kritisk infrastruktur.

GovCERT er placeret i IT- og Telestyrelsen, idet Ministeriet for Videnskab, Teknologi og Udvikling har ressortansvaret for sager vedrørende it-sikkerhed og tillige varetager koordineringen af it- og teleberedskabet. GovCERT er ved udgangen af 2010 blevet fuldt funktionsdygtig. GovCERT kan dog først tilbyde alle de påtænkte ydelser over for de tilsluttede myndigheder, når der med Folketingets vedtagelse af dette lovforslag er tilvejebragt særskilt hjemmel til GovCERT's behandling af personoplysninger indeholdt i pakke- og trafikdata.

GovCERT's formål er at være en varslingstjeneste for internettrusler, og herved medvirke til, at der i staten er overblik over trusler og sårbarheder i tjenester, net og systemer relateret til internettet. GovCERT vurderer løbende det sikkerhedsmæssige risikobillede for statens anvendelse af internettet og varsler myndigheder om internetbaserede sikkerhedshændelser og trusler, og varslingstjenesten vil også tilbyde bistand til at imødegå konsekvenserne af angrebene.

I fuld drift vil GovCERT desuden kunne tilbyde en række ydelser, som samlet set sikrer, at der kan reageres hurtigt og effektivt over for trusler mod it-sikkerheden i primært den danske stat. GovCERT vil således i høj grad kunne medvirke til at begrænse, afkorte og i visse tilfælde forhindre nedbrud i it-infrastrukturen.

Gennem GovCERT og ministeriernes fælles indsats øges sikkerheden for den statslige anvendelse af internettet. GovCERT medvirker til, at staten kan reagere koordineret på trusler mod informationssikkerheden.

GovCERT samarbejder blandt andet med DK-CERT og andre landes nationale CERT'er. DK-CERT (Danish Computer Emergency Response Team) er en tjeneste fra styrelsen UNI-C under Undervisningsministeriet. DK-CERT fungerer som CERT for Forskningsnettet og UNI-C's interne net. GovCERT vil derfor kunne formidle information om internetsikkerhed til myndighederne, der rækker ud over det, der er kommercielt tilgængeligt.

GovCERT's ydelser stilles som udgangspunkt til rådighed for statens institutioner.

Lovforslaget hjemler desuden, at kommuner og regioner samt visse kritiske sektorer (f.eks. finans-, energi-, samt it- og telesektoren) vil kunne tilslutte sig GovCERT.

1.1.2. Internationalt er det erkendt, at det er en vigtig opgave at reducere de risici, der er forbundet med anvendelsen af internettet. En række europæiske lande har således etableret statslige varslingstjenester, som varetager overvågnings- og varslingsopgaver for det statslige område.

Varslingstjenester i de øvrige europæiske lande er typisk karakteriseret ved, at de er statsligt ejet og drevet, og at målgruppen for deres virke er hele staten. For alle varslingstjenester gælder det, at ansvaret og driften er placeret i samme myndighed. Der er dog nationale forskelle på den organisatoriske placering. Hovedparten af varslingstjenesterne er placeret hos civile myndigheder, og der er etableret et tæt samarbejde med sikkerhedsmyndighederne i de pågældende lande.

I Norge blev der i 2000 etableret et Varslingssystem for Digital Infrastruktur (VDI). VDI organiserer og driver et nationalt netværk af indbrudsdetektionssensorer på internettet, som detekterer, om der forsøges udført uønsket aktivitet mod kritisk digital infrastruktur i Norge. VDI omfatter ikke kun de offentlige institutioner, men også en række for samfundet kritiske private virksomheder.

I Sverige er der tilsvarende etableret en national GovCERT, og det er efter norsk forbillede yderligere besluttet at undersøge mulighederne for at udbygge og samordne de eksisterende varslingssystemer.

I Frankrig er GovCERT funktionen varetaget af CERTA, som er en del af det franske militære og civile sikkerhedssystem. CERTA er ansvarlig for at bistå de franske statslige organer med at sikre, at den fornødne informationssikkerhed er til stede, samt hjælpe med at behandle sikkerhedshændelser eller angreb mod statens it-systemer.

1.1.3. GovCERT's ydelser kan grundlæggende opdeles i to hovedgrupper: Ydelser, der tilbydes med henblik på at forebygge alvorlige internetrelaterede sikkerhedshændelser og ydelser, som tilbydes efter en hændelse er indtruffet. De konkrete ydelser er udviklet i en fokusgruppe bestående af Statens It, Udenrigsministeriet og SKAT. Ydelseskataloget har endvidere været forelagt Statens It-sikkerhedsforum, Statens It-forum og Statens It-råd.

1.1.4. GovCERT er etableret i IT- og Telestyrelsen og indgår i IT- og Telestyrelsens sektorberedskab. Beredskabet har til formål at sikre, at samfundsvigtig elektronisk

kommunikation kan finde sted i en beredskabssituation med henblik på, at samfundets funktioner, som måtte være afhængige heraf, så vidt muligt kan opretholdes.

GovCERT's opgaver kan opsummeres således:

- Indhentning af information om sikkerhedshændelser og aktiviteter i net og systemer i staten.
- Analyse og vurdering af internet-sikkerhedsniveauet i staten samt analyse af enkelthændelser.
- Varsling om internet-relaterede sikkerhedshændelser, rådgivning om modforholdsregler og i særlige tilfælde bistand til myndigheder ved omfattende hændelser.
- Kontaktpunkt for tilsvarende varslingstjenester i andre lande og løbende udveksling af information med disse.

GovCERT's opgaver vedrørende varsling og informationsindsamling forudsætter et opdateret og indgående kendskab til situationen på internettet og især den trafik, som er på den danske del af internettet. Dette kendskab tilegnes gennem analyse af pakke- og trafikdata for virus- og hackerangreb.

Det er derfor nødvendigt at etablere et alarmsystem i form af et såkaldt Intrusion Detection System (GovCERT IDS) på udvalgte institutioners internetlinjer. IDS-tjenesten er et tilbud til institutionerne, som er tilsluttet GovCERT. Se mere om GovCERT IDS under 1.2.2.

1.1.5. Da GovCERT vil få kendskab til oplysninger om sårbarheder i it-systemer i staten, er det nødvendigt, at GovCERT klassificerer informationerne i henhold til Statsministeriets sikkerhedscirkulære (cirkulære nr. 204 af 7. december 2001). GovCERTs lokaler og personale er godkendt til at håndtere informationer klassificeret under cirkulæret til niveauet HEMMELIG.

1.2. Varslingstjenestens behandling af personoplysninger

1.2.1. Formålet med lovforslaget er at sikre den nødvendige lovhjemmel til GovCERT's behandling af personoplysninger indeholdt i de indsamlede pakkedata og trafikdata. Behandlingen af personoplysninger er påkrævet for, at varslingstjenestens formål kan opfyldes. Som beskrevet i lovforslagets § 3 og nedenfor er det dog kun i visse

afgrænsede tilfælde, at GovCERT vil få adgang til personoplysninger indeholdt i pakke- og trafikdata. Herudover er det formålet, at både kommuner og regioner samt private virksomheder, der beskæftiger sig med kritisk infrastruktur, kan tilbydes at blive tilsluttet tjenesten.

Begreberne "personoplysning" og "behandling" skal forstås i overensstemmelse med definitionerne i persondatalovens § 3, stk. 1, nr. 1 og 2. I relation til dette lovforslag er det særligt relevant at bemærke, at ip-adresser betragtes som personoplysninger, hvorfor persondataloven også finder anvendelse på trafikdata, som bl.a. omfatter ip-adresser, jf. definitionen heraf i lovforslagets § 2, nr. 2.

GovCERT skal i første række sikre de statslige myndigheder, der vælger at tilslutte sig varslingstjenesten, mod hacker- og virusangreb. Til det formål er der med GovCERT etableret det nævnte alarmsystem (GovCERT IDS), der skal behandle myndighedernes ind- og udgående internettrafik (pakke- og trafikdata). Behandlingen består eksempelvis af en automatisk scanning af internettrafikken efter it-angreb baseret på en angrebssignatur fra kendte it-angreb, og af en manual vurdering af mulige angrebskarakteristika ved begrundet mistanke om it-angreb.

Kommuner og regioner skal også kunne tilslutte sig GovCERT i det omfang, varslingstjenesten har kapacitet hertil. Det er en forudsætning for denne tilslutning, at kommuner og regioner, der vælger at tilslutte sig varslingstjenesten, selv betaler fuldt ud for GovCERT's ydelser i det omfang, kommunernes og regionernes tilslutning ikke er finansieret på anden vis, f.eks. via UMTS-midlerne.

Målet for GovCERT's virke er overordnet via analyse- og varslingsvirksomhed i videst muligt omfang at undgå, at offentlige myndigheder udsættes for både små og mere omfangsrige hacker- og virusangreb.

Ansvaret for den enkelte myndigheds it-sikkerhed ændres ikke som følge af GovCERT's aktiviteter. Det er således fortsat den enkelte myndigheds ansvar at opretholde et passende niveau for it-sikkerhed. GovCERT vil rådgive og bistå de tilsluttede myndigheder i fornødent omfang, uden at der herved ændres ved den eksisterende ansvarsfordeling.

Dele af den kritiske nationale infrastruktur som f.eks. elforsyningen, forestås i dag af private virksomheder. Det samfundsmæssige behov for GovCERT's bistand gør sig også

gældende for disse virksomheder. Lovforslaget indeholder derfor hjemmel til, at disse virksomheder også kan tilslutte sig varslingstjenesten på et senere tidspunkt. Der henvises til de specielle bemærkninger neden for i forbindelse med lovforslagets § 1, stk. 2.

1.2.2. For at nå målet skal GovCERT indhente information om sikkerhedshændelser og aktiviteter i net og systemer hos de tilsluttede myndigheder, ligesom GovCERT skal varsle ved internetrelaterede sikkerhedshændelser samt generelt vurdere sikkerhedsniveauet på internettet. Endelig skal der udarbejdes risikoanalyser. Dette indebærer, at GovCERT har et løbende og indgående kendskab til sikkerhedssituationen på den danske del af internettet.

Forudsætningen for at kunne tilegne sig dette indgående kendskab er, at internettrafikken (pakke- og trafikdata) behandles på såkaldt pakkeniveau for virus- og hackerangreb. Ved pakkeniveau forstås de enkeltdele som internettrafikken nedbrydes i, i forbindelse med datatransmission. Således kan eksempelvis en e-mail bestå af alt fra nogle ganske få til flere tusinde datapakker afhængig af mailens størrelse.

Med henblik på denne behandling af internettrafikken er der med GovCERT etableret det omtalte Intrusion Detection System (IDS).

GovCERT IDS består bl.a. af decentrale IDS-enheder, som placeres på de tilsluttede myndigheders internetforbindelse. Disse enheder analyserer pakke- og trafikdata for angrebsmønstre på internetforbindelsen og lagrer pakke- og trafikdata i maksimalt 14 kalenderdage, dog som udgangspunkt kun i seks kalenderdage. Fristen forlænges til tre år, hvis der er tale om en bekræftet sikkerhedshændelse jf. nedenfor.

Herudover omfatter systemet centrale servere hos GovCERT. Disse anvendes til lagring af pakke- og trafikdata og til analyser og datalagring i et hændelsesregistreringssystem.

Med etableringen af GovCERT IDS vil varslingstjenesten have mulighed for løbende at analysere netværkstrafikken mellem de tilsluttede myndigheder og internettet og herigennem danne sig et normalbillede, hvilket er centralt for GovCERT's virke.

Normalbilledet defineres af GovCERT på grundlag af indsamling af oplysninger i GovCERT IDS, og består eksempelvis af en oversigt over, hvilke ip-adresser der typisk

kommunikeres med, på hvilket tidspunkt, og i hvilket omfang. Hvis der pludselig sker væsentlige ændringer i normalbilledet, som ikke kan begrundes med særlige aktiviteter hos myndigheden selv, vil GovCERT kunne gennemføre tilbundsgående tekniske analyser af pakke- og trafikdata, herunder spore hvorfra eventuel anormal trafik udgår, og vurdere, om hensigten med dette må formodes at være fjendtlig. Et eksempel på anormal trafik kan være, at en myndighed transmitterer store mængder data til en ip-adresse uden for normal arbejdstid, hvortil der ikke plejer at være særlig aktivitet.

De oplysninger, som GovCERT behandler, kan betegnes som pakkedata, trafikdata og alarmer. Alarmer genereres af GovCERT IDS ud fra bestemte trafikmønstre i pakke- og trafikdata.

Pakkedata vil blive slettet umiddelbart efter GovCERT's analyse, hvis denne ikke viser tegn på en sikkerhedshændelse. Analyseret pakkedata vil således kun blive opbevaret, såfremt data er relateret til en konkret sikkerhedshændelse i GovCERT's hændelsesregistreringssystem.

Pakke- og trafikdata, herunder alarmer, der indgår som information i en bekræftet sikkerhedshændelse, opbevares i op til tre år. Trafikdata der ikke er relateret til en bekræftet sikkerhedshændelse gemmes i op til 12 måneder.

Det er centralt at bemærke sig vedrørende de tre nævnte tidsfrister i loven, at der er tale om den maksimale tid, som GovCERT kan opbevare de pågældende oplysninger i. Det følger af persondatalovens § 5, stk. 5, at de oplysninger, som GovCERT indsamler, ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Persondatalovens § 5, stk. 5, har således den konsekvens i forhold til de omtalte tidsfrister for sletning af indsamlede oplysninger, at GovCERT er forpligtet til at slette oplysningerne på et tidligere tidspunkt, hvis varslingstjenestens formål ikke længere gør opbevaringen nødvendig.

Fristerne er i øvrigt fastlagt på baggrund af en it-teknisk vurdering af det nødvendige behov i forbindelse med GovCERT's virke. I forbindelse med denne vurdering er erfaringer fra andre landes CERT'er inddraget. Fristens længde på tre år er valgt for at kunne

sammenholde angreb med tidligere angreb inden for en teknologisk relevant periode, da der fortsat ses angreb rettet mod sårbarheder eller konfigurationsfejl, der er flere år gamle. Tre år betragtes som den teknologiske "levealder" for mange it-systemer, hvorefter systemerne må udfases eller gennemgribende opdateres.

1.2.3. GovCERT's formål er ikke at indsamle personoplysninger. Som følge af den oven for beskrevne rent tekniske behandling af pakke- og trafikdata med henblik på varslingsopgaven indebærer GovCERT's aktiviteter dog uundgåeligt også behandling af personoplysninger, herunder indsamling og opbevaring af personoplysninger.

Den beskrevne behandling af personoplysninger i forbindelse med indsamlingen af de tilsluttede myndigheders ind- og udgående internettrafik (pakke- og trafikdata) er således en uundgåelig konsekvens af GovCERT's arbejde med løbende at vurdere it-sikkerheden og varsle myndigheder om sikkerhedshændelser og trusler på internettet.

Formålet med dette lovforslag er således at tilvejebringe den anbefalede særskilte lovhjemmel for GovCERT's behandling af personoplysninger.

2. GÆLDENDE RET

2.1.1. Lov om behandling af personoplysninger (persondataloven) gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, jf. lovens § 1, stk. 1.

"Personoplysninger" og "behandling" er defineret i persondatalovens § 3, stk. 1, nr. 1 og 2. Begreberne skal forstås i overensstemmelse med disse definitioner.

Persondatalovens § 5 indeholder en række grundlæggende principper for den dataansvarliges behandling af oplysninger, herunder regler om indsamling, ajourføring og opbevaring mv. Behandling af oplysninger skal ske i overensstemmelse med "god databehandlingsskik", jf. § 5, stk. 1. Dette indebærer, at behandlingen skal være rimelig og lovlig.

Indsamling af oplysninger må endvidere kun ske til udtrykkeligt angivne og saglige formål, og senere behandling af oplysningerne må ikke være i strid med disse formål, jf. § 5, stk. 2.

I kravet om udtrykkelighed ligger, at den dataansvarlige i forbindelse med indsamlingen skal angive et formål, som er tilstrækkeligt veldefineret og velafgrænset til at skabe åbenhed og klarhed omkring behandlingen, og at formålet skal defineres med en vis præcision. I kravet om saglighed ligger, at en indsamling skal ske til løsning af en opgave, som det ligger inden for den offentlige myndigheds område at varetage, henholdsvis inden for den (lovlige) virksomhed, som den private foretager.

Efter § 5, stk. 3, skal de oplysninger, som behandles, være relevante og tilstrækkelige og må ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles. Bestemmelsen indeholder et proportionalitetsprincip, hvorefter behandling af personoplysninger ikke må gå videre, end hvad der kræves til opfyldelse af de formål, som den dataansvarlige er berettiget til at forfølge. Om betingelsen om proportionalitet er opfyldt må vurderes ud fra den konkrete sammenhæng, hvori oplysningerne behandles.

Det følger af persondatalovens § 5, stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

2.1.2. Persondatalovens §§ 6-8 indeholder en række bestemmelser om, hvornår indsamling, registrering og videregivelse af personoplysninger kan ske (behandlingsregler). GovCERT's aktiviteter vil kun kunne udøves, hvis disse betingelser er opfyldt.

Efter persondatalovens § 6, stk. 1, nr. 1-7, kan behandling af almindelige, ikke-følsomme personoplysninger (dvs. alle andre oplysninger end følsomme oplysninger omfattet af lovens §§ 7 og 8) ske, hvis den registrerede har givet udtrykkeligt samtykke, eller hvis behandlingen er nødvendig af nærmere angivne grunde, herunder for at udføre en opgave i samfundets interesse eller for at udføre offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Efter persondatalovens § 7, stk. 1, gælder et almindeligt forbud mod behandling af oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold samt oplysninger om helbredsmæssige og seksuelle forhold. § 7, stk. 2-6, indeholder dog visse undtagelser hertil. Behandling kan f.eks. ske, hvis den er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares (stk. 2, nr. 4). Efter § 7, stk. 2, nr. 4, kan behandlingen ske i den dataansvarliges, den registreredes eller i tredjemands interesse. Bestemmelsen omfatter bl.a. offentlige myndigheders behandling af oplysninger som led i myndighedsudøvelse.

Efter persondatalovens § 8 gælder der særlige behandlingsregler med hensyn til oplysninger om strafbare forhold, væsentlige sociale problemer og lignende følsomme privatlivsforhold. Sådanne oplysninger må kun behandles, hvis betingelserne i lovens § 7 er opfyldt. Ud over, hvad der følger af § 7, kan en offentlig forvaltningsmyndighed behandle oplysninger om strafbare forhold, væsentlige sociale problemer og lignende følsomme privatlivsforhold, hvis det er nødvendigt for at varetage den pågældende myndigheds opgaver.

2.1.3. Persondatalovens kapitel 8-10 indeholder en række regler om den registreredes rettigheder, som bl.a. omfatter ret til information om, at der indsamles oplysninger om den pågældende, jf. lovens §§ 28 og 29.

Efter § 29, stk. 1, påhviler det som udgangspunkt den dataansvarlige at oplyse om sin identitet og formålet med behandlingen mv. Det gælder dog ikke, hvis den registrerede allerede er bekendt med oplysningerne, hvis registreringen eller videregivelsen af oplysninger udtrykkeligt er fastsat ved lov, eller hvis underretning af den registrerede viser sig umulig eller uforholdsmæssigt vanskelig. Oplysningspligten kan endvidere begrænses i medfør af lovens § 30, hvis det f.eks. er nødvendigt af hensyn til forebyggelse og efterforskning af straffesager.

Den registrerede har endvidere ret til indsigt i de oplysninger, der behandles om den pågældende, og har bl.a. ret til at gøre indsigelse mod, at behandling finder sted, at få korrigeret eller slettet oplysninger, der er urigtige eller vildledende, og at klage til Datatilsynet, jf. lovens §§ 31-35 og 37-40.

2.1.4. Persondatalovens §§ 41 og 42 omhandler fortrolighed og datasikkerhed. Den dataansvarlige skal iværksætte de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Relevante sikkerhedstiltag kan f.eks. være fysisk sikring af datamedier, adgangskontrol og brug af password samt uddannelse og instruktion.

For offentlige myndigheders behandling af personoplysninger gælder både persondatalovens regler om datasikkerhed og den i medfør heraf udstedte sikkerhedsbekendtgørelse, jf. bekendtgørelse nr. 528 af 15. juni 2000 med senere ændringer om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

2.1.5. Datatilsynet har til opgave at føre tilsyn med persondatalovens overholdelse, behandle klager fra registrerede personer samt afgive udtalelser og udstede tilladelser i forbindelse med anmeldelse af behandlinger til tilsynet, jf. lovens §§ 57-64.

Efter persondatalovens § 62, stk. 2, har Datatilsynet mulighed for at foretage inspektioner (kontrolbesøg) hos bl.a. offentlige myndigheder.

3 LOVFORSLAGETS INDHOLD

3.1. Tilslutning til varslingstjenesten

GovCERT bygger på, at offentlige myndigheder – først og fremmest statslige – tager stilling til, om myndigheden vil tilslutte sig den statslige varslingstjeneste for internettrusler. Lovforslaget lægger som beskrevet oven for op til at også andre – kommunale og regionale myndigheder samt private virksomheder beskæftiget med kritisk infrastruktur – vil kunne få mulighed for at vælge at tilslutte sig.

3.2. Automatisk indsamling af personoplysninger

3.2.1. Det er hensigten med lovforslaget, at den form for behandling af personoplysninger, som GovCERT's aktiviteter vil medføre, skal anskues som GovCERT's indsamling af oplysninger og ikke som videregivelse af oplysninger fra de tilsluttede myndigheder til GovCERT.

Det anførte gælder navnlig som følge af, at GovCERT selv opstiller de omtalte decentrale IDS-enheder, som placeres uden for de tilsluttede myndigheders interne netværk, og

fordi GovCERT herefter automatisk i IDS-enhederne modtager oplysninger om ind- og udgående internettrafik (pakke- og trafikdata).

Det anførte medfører, at GovCERT ved den automatiske indsamling af personoplysninger ikke skal opfylde de af persondatalovens regler, der alene vedrører den form for behandling af personoplysninger, der beskrives som videregivelse. Se i øvrigt om GovCERT's videregivelse af indsamlede oplysninger neden for under punkt 3.3.

3.2.2. GovCERT bygger på en forudsætning om, at der ikke kan eller vil blive indhentet samtykke til GovCERT's behandling af personoplysninger, da GovCERT's indsamling af bl.a. personoplysninger som nævnt sker automatisk.

3.3. Adgang til trafik- og pakkedata

Lovforslaget indebærer, at GovCERT får adgang til såvel trafikdata som pakkedata. Det skal i den forbindelse særligt overvejes, hvorvidt det er nødvendigt og proportionalt, at GovCERT har adgang til at kigge i pakkedata ved sikkerhedshændelser, eller om formålet med GovCERT kunne imødekommes alene ved adgang til trafikdata eller med en anden teknisk indretning af GovCERT's systemer. Såfremt det konkluderes, at adgang til pakkedata er nødvendigt og proportionalt, skal det efterfølgende vurderes, i hvilket omfang, der skal gives adgang til pakkedata. Der skal være den fornødne proportionalitet mellem adgangen til pakkedata og hensynet til privatlivets fred. Denne proportionalitetsafvejning er afspejlet i lovforslagets § 3, stk. 1, og uddybes nedenfor.

IDS-alarmsystemet, som etableres som led i GovCERT's virke, holder via en lokal elektronisk alarmenhed, opsat hos de tilsluttede offentlige myndigheder, øje med internettrafikken (pakke- og trafikdata). Alarmenheden registrer al ind- og udgående internettrafik – både pakkedata og trafikdata. Enheden sender dog kun data til GovCERT ved mistanke om en sikkerhedshændelse.

Hvis GovCERT kun får adgang til at behandle trafikdata identificeres blot mulige tegn på it-angreb. Angrebets indhold og karakter kan ikke nærmere analyseres og beskrives ud fra trafikdata, og de relevante modforanstaltninger kan dermed ikke besluttes.

For at GovCERT skal kunne yde en proaktiv og reaktiv indsats for sikkerheden på internettet og være i stand til at varsle om it-angreb, således at angrebskilden kan fjernes, inden skadesvirkningen spredes, er det nødvendigt at have adgang til de

pakkedata, som er relateret til den pågældende sikkerhedshændelse. Herved vil det kunne fastslås, hvorvidt dokumenter, e-mails med videre er blevet kopieret og videresendt fra brugerkredsen, og i givet fald hvilke dokumenter. Skadevirkningen kan herefter fastslås, og de relevante modforanstaltninger besluttes.

For eksempel kan en e-mail med et virusinficeret PDF-dokument omgå både antivirusprogrammer og firewall hos en myndighed og herefter kopiere og sende dokumenter fra den inficerede PC tilbage til hackeren uden myndighedens vidende. Hvis GovCERT ikke har adgang til pakkedata, vil GovCERT ikke kunne analysere denne virus og træffe de relevante modforanstaltninger sammen med den berørte myndighed. Hertil kommer, at det ikke uden adgang til pakkedata vil være muligt for GovCERT at fastslå konsekvenserne for den berørte myndighed af et vellykket it-angreb.

De nødvendige oplysninger til brug for effektiv analyse og håndtering af angreb ligger således i pakkedata, og GovCERT vil ikke kunne håndtere kritiske it-angreb på betryggende vis uden adgang til pakkedata.

Efter denne overordnede vurdering af, at det er nødvendigt og proportionalt at give GovCERT adgang til pakkedata, skal det vurderes, i hvilket omfang GovCERT skal have adgang til pakkedata. Der er lagt op til, at pakke- og trafikdata, som knytter sig til en konkret sikkerhedshændelse, kan opbevares i tre år. Pakkedata, der ikke er knyttet til en konkret sikkerhedshændelse, kan maksimalt lagres i 14 kalenderdage. Som udgangspunkt vil pakkedata dog kun blive opbevaret i seks kalenderdage. Trafikdata, som ikke knytter sig til en konkret sikkerhedshændelse, kan maksimalt opbevares i 12 måneder. Det er vigtigt at være opmærksom på, at fristerne alle er maksimumfrister. GovCERT vil løbende være forpligtet til at slette data, som ikke længere er relevante for GovCERT's virke, uanset at fristerne beskrevet i § 3 ikke er overskredet. Derudover er det i § 3 fastsat, at indsamlede pakkedata kun vil kunne blive analyseret af GovCERT, hvis der er begrundet mistanke om en sikkerhedshændelse, og at det kun er den relevante del af de indsamlede data, som kan analyseres.

I hvilket omfang der skal gives adgang til pakkedata vil – udover disse generelle frister for opbevaring - desuden skulle vurderes i den enkelte konkrete sag ved en alarm om en sikkerhedshændelse.

Det er med GovCERT's alarmsystem pt. ikke muligt at foretage en teknisk graduering af adgangen til pakkedata på en sådan måde, at der f.eks. kun gives adgang til visse dele af indholdet af en e-mail. Der kan kun skelnes mellem adgang til pakkedata eller adgang til trafikdata. GovCERT vil imidlertid følge mulighederne tæt for at finde en teknisk løsning herpå.

Længden af fristerne i § 3 er fastsat på baggrund af en proportionalitetsafvejning af hensynet til GovCERT's virke set i forhold til hensynet til privatlivets fred. Det er i visse situationer væsentligt for GovCERT at kunne sammenholde nyindsamlede data med ældre data for f.eks. at kunne analysere et it-angreb nærmere. Heroverfor står hensynet til de berørte borgeres privatliv. Denne afvejning har resulteret i de nævnte frister, som også er fastsat under inddragelse af erfaringer fra andre landes CERT'er.

3.4. Videregivelse af oplysninger

3.4.1. Det følger af den foreslåede bestemmelse i § 5, at den statslige varslingstjeneste kan videregive pakkedata og trafikdata, der knytter sig til en konkret sikkerhedshændelse, til politiet. Formålet hermed er at sikre, at politiet kan modtage oplysninger til brug for efterforskning og forfølgelse af strafbare forhold, der kan være begået i forbindelse med en konkret sikkerhedshændelse, som f.eks. et virusangreb.

GovCERT vil dog have behov for en videre adgang til at udveksle trafikdata, herunder ip-adresser, til andre myndigheder og tilsluttede private virksomheder ved varsling eller i tilfælde af konkrete sikkerhedshændelser. Videregivelsen skal sikre, at myndighederne og de pågældende virksomheder kan iværksætte lokale modforanstaltninger over for hændelsen. Det kan for eksempel være blokering af kommunikation med en specifik ip-adresse.

Der henvises i øvrigt til de specielle bemærkninger nedenfor vedrørende lovforslagets § 5.

3.4.2. GovCERT vil i øvrigt have behov for at udveksle ip-adresser og anden trafikdata med tilsvarende varslingstjenester i andre lande i forbindelse med konkrete sikkerhedshændelser på internettet. GovCERT kan ikke videregive indholdet af en e-mail (pakkedata) eller andre personfølsomme oplysninger.

Videregivelse af trafikdata er vigtigt for GovCERT's virke. Derved kan en CERT i et andet land f.eks. anmode den lokale internetudbyder om nedtagning af den angribende ip-

adresse. Tilsvarende er det vigtigt, at GovCERT modtager trafikdata fra udenlandske CERT'er til forebyggelse af et it-angreb.

International koordination af forsvar mod elektroniske angreb i form af udveksling af ip-adresser og anden trafikdata er dermed en væsentlig del af grundlaget for GovCERT's aktiviteter.

3.5. Uafhængigt tilsyn

For at sikre at GovCERT's behandling af personoplysninger er i overensstemmelse med dette lovforslag og gældende ret i øvrigt, indeholder lovforslaget en bestemmelse om, at ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, som skal følge GovCERT's virksomhed. Tilsynet vil blandt andet kunne bestå i en årlig afrapportering til ministeren for videnskab, teknologi og udvikling om GovCERT's virksomhed.

3.6. Forholdet til persondataloven

3.6.1. Det er nødvendigt for, at GovCERT kan danne det for varslingsopgaven helt centrale normalbillede for internettrafikken (pakke- og trafikdata), at al ud- og indgående internettrafik fra en tilsluttet myndighed indsamles.

Det er uundgåeligt, at nogle af de personoplysninger, som GovCERT – som følge af systemets opbygning – behandler, vil indeholde både almindelige, ikke-følsomme oplysninger (persondatalovens § 6), og følsomme personoplysninger (§§ 7 og 8). Disse oplysninger kan forekomme f.eks. i ukrypterede e-mails fra borgere til ansatte i de tilsluttede myndigheder.

GovCERT's behandling af personoplysningerne skal opfylde persondatalovens § 5, der indeholder en række grundlæggende principper for den behandling af personoplysninger, som den dataansvarlige – her GovCERT – foretager.

Kravet om god databehandlingsskik i persondatalovens § 5, stk. 1, indebærer, at medarbejderne hos de myndigheder, som bliver omfattet af GovCERT's behandlinger, skal have klar og tydelig forudgående information om, at al brug af internettet, herunder e-mails, vil blive behandlet, herunder eventuelt gennemset og opbevaret med de formål, som varetages af GovCERT.

I forhold til saglighedskravet i § 5, stk. 2, vil det eksempelvis være i strid med bestemmelsen, hvis GovCERT's personale i forbindelse med den beskrevne analyse af

internettrafikken behandler personoplysninger, uden at det sker i forbindelse med forfølgelsen af det saglige formål med bl.a. at begrænse og varsle om hacker- og virusangreb. GovCERT skal således sikre, at behandlingen af personoplysninger ikke sker i videre omfang end dette formål tilsiger.

Vedrørende kravet i persondatalovens § 5, stk. 2, om formålsbestemthed bemærkes, at den foreslåede ordning netop går ud på (alene) at give GovCERT adgang til at udføre varslingsopgaven bl.a. med henblik på at begrænse hacker- og virusangreb.

Det må dog nøje overvejes, hvorvidt en senere brug af de behandlede oplysninger er uforenelig med det oprindelige formål med indsamlingen af oplysningerne. Formålet, hvortil de indsamlede oplysninger må anvendes, bør derfor fastlåses til alene at være GovCERT's egne oprindelige formål.

Disse overvejelser har resulteret i lovforslagets § 5, hvorefter der alene kan ske videregivelse til politiet af pakkedata og trafikdata, som knytter sig til en konkret sikkerhedshændelse.

Derudover indebærer lovforslagets § 5, nr. 2, at GovCERT som led i aktiviteterne skal have mulighed for at overføre trafikdata til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande i henhold til varslingstjenestens formål. Her er overførselsmuligheden således begrænset til trafikdata, hvorfor f.eks. indhold af e-mails ikke vil kunne overføres. Se endvidere under 3.3.

Der henvises i øvrigt til de specielle bemærkninger nedenfor vedrørende lovforslagets § 5.

I forhold til persondatalovens § 5, stk. 3, og spørgsmålet om proportionalitet, indebærer bestemmelsen, at GovCERT's aktiviteter skal gennemføres på en sådan måde, at de virker mindst muligt integritetskrænkende for den almindelige borger således, at det i videst muligt omfang undgås, at personoplysninger behandles, herunder ikke mindst, at indholdet af e-mails ikke behandles.

Ud over de generelle betingelser i persondatalovens § 5 skal betingelserne i persondatalovens §§ 6-8 være opfyldt.

Det er et krav i bestemmelserne, at behandling (uden samtykke) skal være nødvendig. Der er i den forbindelse overladt den dataansvarlige et vist skøn. Denne vurdering skal i første omgang foretages af IT- og Telestyrelsen som dataansvarlig myndighed.

Selve den beskrevne indsamling af al ind- og udgående internettrafik og de deri indeholdte personoplysninger vil have den fornødne hjemmel i persondatalovens §§ 6-8. Der findes således i persondatalovens § 6, stk. 1, § 7, stk. 2, og § 8, stk. 1 og 6, mulighed for, at en offentlig myndighed som IT- og Telestyrelsen (GovCERT) kan behandle personoplysninger uden samtykke fra de registrerede.

Jo mere indgribende den efterfølgende behandling af personoplysningerne kan siges at være, jo strengere krav stilles der til opfyldelsen af det nødvendighedskrav, der ligger i persondatalovens §§ 6-8 og til opfyldelsen af de beskrevne principper i § 5.

GovCERT vil skulle vurdere opfyldelsen af disse regler løbende i det daglige arbejde. GovCERT vil således kun kunne behandle og eventuelt nærmere analysere en e-mailkorrespondance, når det er nødvendigt af hensyn til opfyldelsen af varslingsopgaven, herunder håndteringen af hackerangreb.

Til gengæld vurderes det, at der i disse undtagelsesvise situationer vil være hjemmel til den behandling af personoplysninger, som opgaven nødvendigvis medfører, inden for rammerne af persondatalovens behandlingsregler.

Der er i øvrigt ingen grund til at antage, at vurderingen af nødvendigheden og proportionaliteten i forbindelse med GovCERT's behandling af personoplysninger efter persondatalovens §§ 5-8 vil falde anderledes ud efter persondataloven end den tilsvarende vurdering, som foretages neden for i afsnit 3.7 vedrørende forholdet til Den Europæiske Menneskerettighedskonventions artikel 8.

Disse regler i persondataloven er i forhold til GovCERT's aktiviteter afspejlet i lovforslagets § 3, stk. 1, 2. pkt.

Sammenfattende er det således muligt for GovCERT som dataansvarlig i forbindelse med udøvelsen af aktiviteterne at sikre, at beskyttelsen i persondatalovens § 5-8 også respekteres.

3.6.2. I forhold til persondatalovens kapitel 8 om den dataansvarliges oplysningspligt over for den registrerede kan det nævnes, at GovCERT's indsamling af oplysninger – i lighed med det for tv-overvågning gældende – skal anses for at være foretaget hos andre end den registrerede, jf. persondatalovens § 29, stk. 1.

Der påhviler derfor som udgangspunkt IT- og Telestyrelsen som dataansvarlig en oplysningspligt over for de registrerede efter persondatalovens § 29, stk. 1, men der vil normalt kunne gøres undtagelse herfra, da opfyldelse af oplysningspligten normalt vil være umulig eller uforholdsmæssig vanskelig efter persondatalovens § 29, stk. 3.

3.6.3. For så vidt angår indsigtsretten efter persondatalovens § 31 bemærkes, at der kan gøres undtagelse herfra i samme omfang som efter reglerne i bl.a. offentlighedslovens § 14, jf. persondatalovens § 32, stk. 2. Som følge af den særlige bestemmelse om tavshedspligt, som pålægges GovCERT's personale ved lovforslagets § 4, stk. 2, i overensstemmelse med offentlighedslovens § 14, er de personoplysninger, som GovCERT behandler i forbindelse med sit virke, undtaget fra indsigtsretten efter persondatalovens § 32, stk. 2.

3.6.4. For så vidt angår retten til at gøre indsigelse, jf. persondatalovens § 35, åbner persondatadirektivets artikel 14, stk. 1, litra a, mulighed for, at det kan bestemmes ved lov, at retten til at gøre indsigelse afskæres. På den baggrund er der indsat en undtagelsesbestemmelse i de vedlagte lovforslag, som lægger op til, at persondatalovens § 35 ikke skal finde anvendelse på GovCERT's aktiviteter. Det vil medføre, at registrerede ikke vil kunne gøre indsigelse over for GovCERT's behandling af personoplysninger.

En registreret kan dog fortsat klage til Datatilsynet over GovCERT's behandling af personoplysninger vedrørende den pågældende, jf. persondatalovens § 40 og kapitel 16.

3.7. Forholdet til grundlovens § 72

Grundlovens § 72 har følgende ordlyd: "Boligen er ukrænkelig. Husundersøgelse, beslaglæggelse og undersøgelse af breve og andre papirer samt brud på post-, telegraf- og telefonhemmeligheden må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse."

Det antages i den juridiske litteratur, at indholdet af e-mails også er omfattet af grundlovens beskyttelse af meddelelseshemmeligheden (brud på post-, telegraf- og

telefonhemmeligheden). En myndigheds brud på meddelelseshemmeligheden forudsætter uden for strafferetsplejens område som udgangspunkt dels en udtrykkelig lovhjemmel og dels en forudgående retskendelse i det konkrete tilfælde, med mindre der også foreligger en udtrykkelig lovhjemmel til at undtage kravet om retskendelse. Retskendelse behøves heller ikke i situationer, hvor den, som foranstaltningen vedrører, giver samtykke til, at undersøgelsen bliver foretaget.

Den foreslåede ordning går ud på, at GovCERT skal behandle, herunder efter omstændighederne analysere, tilsluttede myndigheders og private virksomheders ind- og udgående trafik- og pakkedata. GovCERT skal i den forbindelse i et vist omfang have ret til at skaffe sig adgang til pakkedata, eksempelvis indholdet af e-mails.

Ordningen efter lovforslaget vil uundgåeligt i visse tilfælde indebære et indgreb i meddelelseshemmeligheden i grundlovens forstand. Der vil dog i vidt omfang foreligge et samtykke, som indebærer, at det ikke vil være nødvendigt at indhente retskendelse efter grundlovens § 72. Der vil imidlertid også forekomme tilfælde, hvor et sådant samtykke ikke foreligger, og eftersom det i praksis ikke vil være muligt at indhente en retskendelse, indeholder lovforslaget på den baggrund en undtagelse fra grundlovens § 72's krav herom.

Videnskabsministeriet har bl.a. af hensyn til grundlovens § 72 overvejet nødvendigheden og proportionaliteten af den foreslåede ordning. Der henvises i den forbindelse til bemærkningerne ovenfor under pkt. X.X, hvoraf det fremgår, at der med lovforslaget er fundet den påkrævede proportionalitet mellem hensynet til GovCERT's formål og hensynet til privatlivets fred for de berørte borgere.

3.8. Forholdet til Den Europæiske Menneskeretskonvention

Efter Den Europæiske Menneskerettighedskonventions artikel 8, stk. 1, har enhver ret til respekt for sit privatliv og familieliv.

Beskyttelsen efter artikel 8 omfatter såvel indgreb i meddelelseshemmeligheden, f.eks. overvågning af e-mailkorrespondance og internettrafik, som offentlige myndigheders indsamling, opbevaring og anvendelse mv. af personoplysninger generelt.

Indgreb i kommunikation via bl.a. e-mails vil som udgangspunkt udgøre et indgreb efter EMRK artikel 8. Hvis en offentlig arbejdsgiver overvåger en ansats brug af e-mail og

internet, vil det således udgøre et indgreb i den ansattes ret til privatliv og korrespondance, når den ansatte med rimelighed kunne forvente ikke at blive overvåget (se Copland mod Storbritannien, dom af 3. april 2007, præmis 41-42).

Det samme vil være tilfældet, hvor en arbejdsgiver tillader en (anden) myndighed at overvåge den ansattes brug af e-mail og internet.

Det forudsættes imidlertid, at den ansatte i forbindelse med afsendelse af privat e-mail giver samtykke til GovCERT-behandlingen. Når det er op til myndighedens personalepolitik, om medarbejderne må sende eller modtage privat e-mail, må myndigheden således også kunne fastsætte, at medarbejderne kun må sende privat e-mail mod at samtykke til GovCERT-behandlingen. Det antages på den baggrund, at iværksættelsen af overvågningen af udgående e-mails med privat indhold ikke i sig selv vil udgøre et indgreb i rettighederne efter EMRK artikel 8.

For så vidt angår indgående private e-mails samt offentlige myndigheders indsamling, opbevaring og anvendelse mv. af personoplysninger vil der derimod være tale om et indgreb i borgernes ret til privatliv.

Da det som følge af den oven for beskrevne tekniske opbygning af GovCERT ikke kan udelukkes, at GovCERT vil behandle personoplysninger om en persons privatliv, må aktiviteterne anses for et indgreb i retten til respekt for privatlivet, jf. konventionens artikel 8, stk. 1.

Det følger herefter af konventionens artikel 8, stk. 2, at et sådant indgreb kun kan foretages, hvis det er foreskrevet ved lov og er nødvendigt i et demokratisk samfund til varetagelse af nærmere bestemte anerkendelsesværdige formål.

Med den foreslåede lov vil der blive klar lovhjemmel for GovCERT's aktiviteter, som bygger på en legitim og helt åbenlys (samfundsmæssig) interesse i at håndtere sikkerhedshændelser af it-mæssig karakter for offentlige myndigheder i Danmark.

Indgrebet i privatlivet skal herudover efter artikel 8, stk. 2, have et sagligt formål og være proportionalt.

GovCERT har til formål gennem analyse, information, varsling og koordination at mindske konsekvenserne af sikkerhedshændelser på internettet. GovCERTs aktiviteter tilsigter således at beskytte den nationale sikkerhed, den offentlige tryghed og landets økonomiske velfærd samt andres rettigheder og friheder. Formålet må således anses for sagligt.

IT- og Telestyrelsens rapport om varsling af internettrusler fra 2007 konkluderede, at der i Danmark er behov for en særskilt tjeneste til at håndtere sådanne sikkerhedshændelser for det danske samfund som et led i den nationale it-sikkerhedsstrategi. Den varslingsopgave mv., som er tiltænkt GovCERT, må således siges at være både egnet til og nødvendig for at nå det beskrevne saglige mål om at forhindre hacker- og virusangreb mv.

Der kan i den forbindelse også henvises til de neden for i afsnit 8.1.1 beskrevne signaler fra EU-Kommissionen og Rådet om, at oprettelsen af statslige it-beredskabsenheder (″GovCERT′er″) er en måde, hvorpå medlemsstaterne kan løse de notoriske trusler mod deres it-sikkerhed.

Den samfundsmæssige interesse i at forhindre og håndtere sikkerhedshændelser af it-mæssig karakter for offentlige myndigheder i Danmark må således anses at overstige hensynet til privatlivet for de personer, om hvilke GovCERT behandler personoplysninger. Aktiviteterne er endvidere begrænset til de tilsluttede myndigheder og virksomheders ind- og udgående data.

GovCERT′s formål er endvidere som nævnt ikke i sig selv at indsamle personoplysninger. Indsamlingen er i stedet en uundgåelig konsekvens af varslingsopgaven. GovCERT vil i øvrigt kun opbevare oplysningerne, så længe opbevaringen er nødvendig i forhold til varslingsopgaven, hvilket vurderes til tidsmæssigt at være de oven for i afsnit 1.2. beskrevne tidsfrister.

Personoplysningerne vil derudover heller ikke blive offentliggjort; tværtimod er opbevaringen af oplysningerne underlagt strenge sikkerhedsforanstaltninger, så bl.a. offentliggørelse undgås.

Hertil kommer i øvrigt, at GovCERT efter lovforslagets § 6 vil blive underlagt kontrol af et uafhængigt tilsyn. Tilsynets tilstedeværelse vil være med til at sikre, at GovCERT′s behandling af personoplysninger foregår på en retssikkerhedsmæssigt betryggende måde.

Sammenfattende er det opfattelsen, at den behandling af personoplysninger, som er en nødvendig del af GovCERT's aktiviteter vil opfylde betingelserne i artikel 8, stk. 2, i Den Europæiske Menneskerettighedskonvention.

4 DE ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER FOR DET OFFENTLIGE

Regeringen besluttede i forbindelse med oprettelsen af den danske GovCERT, at opgaverne skal finansieres inden for Ministeriet for Videnskab, Teknologi og Udviklings eksisterende ramme. I efteråret 2009 blev det i forbindelse med udmøntningen af UMTS-midlerne besluttet at give yderligere midler til udvidelse af GovCERT's dækningsområde for perioden 2010 til 2012.

I den UMTS-finansierede periode vil ministeriet udvide dækningen i et nærmere bestemt omfang til også at omfatte kommuner, regioner og visse kritiske sektorer (f.eks. finans-, energi-, samt it- og telesektoren) samt information rettet mod borgere, små og mellemstore virksomheder. GovCERT vil for det udvidede dækningsområde køre et testforløb med fem kommuner eller regioner, som vil blive finansieret via UMTS-midlerne. Alle øvrige varslings- og overvågningsaktiviteter i det udvidede dækningsområde vil blive gebyrfinansieret.

Tilsluttede statslige institutioner vil blive tilbudt en alarmenhed. Ønskes yderligere alarmenheder opstillet vil der skulle betales gebyr herfor.

5 DE ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER FOR ERHVERVSLIVET

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet, idet tilslutning til GovCERT er frivillig. Tilsluttede private virksomheder beskæftiget med kritisk infrastruktur vil dog kunne have begrænsede omkostninger afhængig af tilslutningens karakter.

6 DE ADMINISTRATIVE KONSEKVENSER FOR BORGERNE

Lovforslaget har ingen administrative konsekvenser for borgerne.

7 DE MILJØMÆSSIGE KONSEKVENSER

Lovforslaget har ingen miljømæssige konsekvenser.

8 FORHOLDET TIL EU-RETTEN

Lovforslaget er ikke udtryk for implementering af EU-regulering. Lovforslaget indeholder dog regler af relevans for to EU-direktiver.

8.1.1. Der er på EU-niveau foretaget en række overvejelser – der i høj grad svarer til overvejelserne bag iværksættelsen af GovCERT – vedrørende behovet for, at medlemsstaterne iværksætter en eller anden form for statslig overvågningstjeneste for internettrusler.

EU-Kommissionen vedtog således den 30. marts 2009 en meddelelse om beskyttelse af kritisk informationsinfrastruktur med undertitlen "Beskyttelse mod storstilede cyber-angreb og sammenbrud: øget beredskab, sikkerhed og robusthed", jf. KOM (2009) 149 endelig.

I denne handlingsplan opfordrer Kommissionen således medlemsstaterne til bl.a. at oprette "landsdækkende statslige CERT-enheder" og sikre, at disse GovCERT'er "fungerer som nøglekomponent i det nationale beredskab og i informationsudveksling, koordinering og reaktion på sikkerhedshændelser".

Der kan i den forbindelse bl.a. også henvises til Rådets resolution af 18. december 2009 om en samordnet europæisk strategi for net- og informationssikkerhed (EUT 2009/C 321/01).

EU har ikke ønsket at fastlægge det nærmere indhold af de statslige varslingstjenester. Hvordan medlemsstaterne organiserer CERT'erne er således tilsyneladende op til medlemsstaterne selv, men under alle omstændigheder opfordrer EU medlemsstaterne til at oprette bl.a. varslingstjenester som GovCERT.

8.1.2. Persondatadirektivet (direktiv 95/46/EF med senere ændringer) er gennemført i dansk ret med persondataloven.

Persondatadirektivet må anses for at omfatte GovCERT's aktiviteter, i det omfang disse inkluderer behandling af personoplysninger.

Da lovforslaget i videst muligt omfang er indrettet i overensstemmelse med persondataloven, vil Danmarks forpligtelser efter persondatadirektivet ikke blive beskrevet detaljeret i det følgende.

I de tilfælde, hvor lovforslaget er udtryk for en undtagelsesvis fravigelse af persondataloven, er der oven for i afsnit 3.5.4 nærmere redegjort for, hvorfor lovforslaget er i overensstemmelse med persondatadirektivet.

Det vurderes således, at lovforslaget ligger inden for rammerne af persondatadirektivet.

8.1.3. Det generelle persondatadirektiv er suppleret af det specifikke direktiv om elektronisk kommunikation – herefter e-databeskyttelsesdirektivet (direktiv 2002/58/EF med senere ændringer). E-databeskyttelsesdirektivet blev således vedtaget for at supplere persondatadirektivet med en række særlige bestemmelser inden for den elektroniske kommunikation.

E-databeskyttelsesdirektivet finder anvendelse på behandling af personoplysninger i forbindelse med brug af internettet (elektronisk kommunikation, herunder internet og e-mails).

Af relevans for GovCERT's aktiviteter, som de er beskrevet i dette lovforslag, henledes opmærksomheden på, at det følger af direktivets artikel 5, stk. 1, at medlemsstaterne skal sikre kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester – dvs. f.eks. ved brug af internettet og e-mails.

Kommunikationshemmeligheden skal både sikres for så vidt angår selve indholdet af kommunikationen og de dermed forbundne trafikdata om brugen af internettet. Det vil f.eks. sige, at afsenderen af en e-mail skal sikres imod, at den opsnappes, åbnes og læses af andre end adressaten.

Som beskrevet oven for ligger det i GovCERT's system, at der nødvendigvis er risiko for, at oplysninger af privat karakter i en e-mail undtagelsesvist kan blive afsløret over for andre end adressaten, nemlig GovCERT's personale, hvilket – selvom det måtte ske sjældent – må siges at være i konflikt med artikel 5, stk. 1, om kommunikationshemmeligheden i e-databeskyttelsesdirektivet. Der henvises i den forbindelse også til afsnit 2.2 oven for vedrørende den tilsvarende problemstilling i forhold til grundlovens § 72.

Efter artikel 15, stk. 1, i e-databeskyttelsesdirektivet er der dog adgang til at indskrænke rækkevidden af direktivet med hensyn til bl.a. kommunikationshemmeligheden, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem.

Direktivets artikel 15 tillader således, at der i national lovgivning fastsættes regler, der indskrænker beskyttelsen af kommunikationshemmeligheden. Betingelsen er imidlertid, at det sker for at varetage et eller flere af de hensyn, der er nævnt i artikel 15, stk. 1, herunder især – i forhold til GovCERT's aktiviteter – hensynet vedrørende uautoriseret brug af det elektroniske kommunikationssystem og den offentlige sikkerhed.

Det vurderes på den baggrund, at den indskrænkning i kommunikationshemmeligheden, som GovCERT's beskrevne aktiviteter måtte medføre, er proportional og i overensstemmelse med e-databeskyttelsesdirektivet, da indskrænkningen indføres for – i direktivets forstand – at undgå uautoriseret brug af det elektroniske kommunikationssystem og beskytte den offentlige sikkerhed.

Det vurderes således, at lovforslaget ligger inden for rammerne i e-databeskyttelsesdirektivet.

9 DE HØRTE MYNDIGHEDER OG ORGANISATIONER MV.

Et udkast til lovforslag har været sendt i høring hos:
AC, BaneDanmark, Beredskabsstyrelsen, Brancheforum Digitale Medier, Dansk Energi, Dansk Erhverv, Danske Regioner, Dansk Industri, Dansk IT, Datatilsynet, Domstolsstyrelsen, Energinet.dk, Energistyrelsen, Finansrådet, Foreningen Danske Olieberedskabslagre, Forbrugerombudsmanden, Forbrugerrådet, Foreningen Danske Internet Medier, Foreningen for Open Source Leverandører i

Danmark, Forsvarets Efterretningstjeneste, FTF, ISP-sikkerhedsforum, IT-Brancheforeningen, ITEK, It-politisk forening, It-sikkerhedskomiteen, Kommunernes Landsforening, Konkurrence- og Forbrugerstyrelsen, LO, Politiets Efterretningstjeneste, PROSA, Rigspolitiet, Rigsrevisionen, Rådet for persondata og informationssikkerhed, Rådet for større IT-sikkerhed, Statens It-forum, Statens It-råd, Telekommunikationsindustrien i Danmark, UNI C (DK-Cert).

10 SAMMENFATTENDE SKEMA

	Positive konsekvenser /mindre udgifter	Negative konsekvenser/ merudgifter
Økonomiske konsekvenser for det offentlige	Ingen	Tilslutningen til den statslige varslingstjeneste er frivillig. De tilsluttede myndigheder kan få øgede udgifter til it-udstyr i mindre omfang.
Administrative konsekvenser for det offentlige	Ingen	Tilslutningen til den statslige varslingstjeneste er frivillig. De tilsluttede myndigheder kan få øgede administrative byrder i mindre omfang.
Økonomiske konsekvenser for erhvervslivet	Ingen	Tilslutningen til den statslige varslingstjeneste er frivillig. Tilsluttede private virksomheder kan få øgede økonomiske udgifter i mindre omfang.
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgere	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget implementerer ikke EU-regulering.	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Den foreslåede bestemmelse angiver, at formålet med lovforslaget er at skabe klare rammer for GovCERT's behandling af personoplysninger indeholdt i de indsamlede pakke- og trafikdata.

Med lovforslagets stk. 2 ønskes indført mulighed for, at også kommuner, regioner og private virksomheder, der beskæftiger sig med kritisk infrastruktur skal kunne vælge at tilslutte sig varslingstjenesten.

Det er hensigten, at kommuner og regioner kun skal kunne tilslutte sig GovCERT, i det omfang varslingstjenesten har kapacitet hertil. Det forudsættes i den forbindelse, at de kommuner og regioner, der vælger at tilslutte sig varslingstjenesten, selv betaler fuldt ud for GovCERT's ydelser i det omfang kommunernes og regionernes tilslutning ikke er finansieret på anden vis, som f.eks. via UMTS-midlerne.

Dele af den kritiske infrastruktur i Danmark er ejet af private virksomheder. Det gælder f.eks. elforsyningen. Dette afføder et samfundsmæssigt behov for, at også sådanne sektorer kan omfattes af GovCERT's dækningsområde for at sikre samfundets samlede sikkerhed og robusthed på internettet. Private virksomheder beskæftiget med kritisk infrastruktur har dermed også mulighed for at anmode om tilslutning til den statslige varslingstjeneste for internettrusler.

Begrebet "kritisk infrastruktur" omfatter her i overensstemmelse med det beredskabsmæssige udgangspunkt de sektorer, der kan siges at forestå vitale samfundsmæssige interesser, hvori samfundet som sådan har interesse i, at disse opretholdes. Eksempler herpå er finans-, energi samt it- og telesektoren. Begrebet skal fortolkes dynamisk og vil således udvikle sig over tid i takt med samfundsudviklingen, som kan gøre det relevant at inddrage nye sektorer i begrebet.

For så vidt angår tilslutningen til GovCERT, kan ministeren for Videnskab, teknologi og udvikling ifølge stk. 3 fastsætte nærmere regler herom. De anførte myndigheder og virksomheder kan herefter vælge at tilslutte sig GovCERT på baggrund af disse regler. De

private virksomheder, der måtte tilslutte sig varslingstjenesten, skal selv finansiere tjenestens ydelser.

Til § 2

Den foreslåede bestemmelse definerer tre centrale begreber i loven.

Pakkedata er i denne lov afgrænset til kun at omfatte indholdet af internetbaseret kommunikation. Begrebet omfatter det semantiske indhold af en internetbaseret kommunikation, herunder indholdet af en e-mailkorrespondance eller indholdet af tilgåede websider, og derudover det tekniske indhold af kommunikationen, som f.eks. HTML- eller XML-koder.

I forbindelse med GovCERT's analyse af sikkerhedshændelser er det primært det tekniske indhold af kommunikationen og ikke det semantiske indhold af kommunikationen, som er interessant for analysen.

Ved trafikdata forstås i denne lov de oplysninger, som beskriver en internetkommunikation, herunder ip-adresser, internetkommunikationens varighed og tidspunkt mv.

Trafikdata er tillige defineret i bekendtgørelse nr. 714 af 26. juni 2008 om udbud af elektroniske kommunikationsnet og – tjenester (udbudsbekendtgørelsen) og identisk i e-databeskyttelsesdirektivet (direktiv 2002/58/EF med senere ændringer) Definitionen af trafikdata i denne lov er justeret i forhold til denne definition. Sidste led i definitionen vedrørende debitering er således udeladt i definitionen af trafikdata i dette lovforslag, idet data vedrørende debitering ikke har relevans for lovforslaget. Derudover er det præciseret, at det alene er internetbaseret kommunikation, som er omfattet af begrebet trafikdata i overensstemmelse med definitionen af pakkedata i denne lov. Der er herudover ikke med dette lovforslag tiltænkt nogen fravigelse af definitionen af trafikdata i e-databeskyttelsesdirektivet og udbudsbekendtgørelsen.

En sikkerhedshændelse defineres ved, at der enten sker en påvirkning af tilgængelighed, integritet eller fortrolighed af information eller tjenester på internettet. Begrebet er defineret i loven med henblik på at præcisere afgrænsningen af de tilfælde, hvor GovCERT har mulighed for at opbevare pakke- og trafikdata i op til tre år.

Til § 3

Det er formålet med den foreslåede bestemmelse, at der tilvejebringes klar lovhjemmel til GovCERT's behandling af personoplysninger i forbindelse med analyse- og varslingsopgaverne, herunder til indsamling, registrering og opbevaring af oplysninger om de tilsluttede myndigheders og virksomheders ind- og udgående internettrafik, dvs. pakke- og trafikdata, med henblik på varetagelsen af varslingsopgaven.

For så vidt angår hjemmearbejdspladser, som medarbejdere i de tilsluttede myndigheder måtte have, indsamler, registrerer og opbevarer GovCERT alene oplysninger om ind- og udgående trafikdata, herunder ip-adresser, men ikke pakkedata.

GovCERT's aktiviteter vil omfatte behandling af bl.a. personoplysninger, således som dette defineres i § 3, nr. 1, i persondataloven. IT- og Telestyrelsen (GovCERT) betragtes i den forbindelse som dataansvarlig, jf. persondatalovens § 3, nr. 4. At aktiviteterne er omfattet af reglen i persondataloven indebærer, at Datatilsynet har fuld inspektionskompetence i forhold til de registrerede og opbevarede oplysninger, jf. persondatalovens § 62, stk. 2, om behandling, der foretages for den offentlige forvaltning, og at bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige sektor, finder anvendelse.

I tilfælde af begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse vil indhold af f.eks. borgeres private e-mails til tilsluttede myndigheder uundgåeligt kunne blive afsløret over for andre end adressaten, nemlig GovCERT's personale. GovCERT's personale vil i forbindelse med alarmer og øvrige sikkerhedshændelser nærmere analyserer pakkedata for den pågældende periode, hændelsen vedrører. Meddelelseshemmeligheden efter grundlovens § 72 kan dermed i disse tilfælde blive brudt.

Når det således af stk. 1 følger, at GovCERT's aktiviteter foretages "uden retskendelse" skyldes det, at der med bestemmelsen, udover at skabe en klar hjemmel for de undtagelsesvise brud på meddelelseshemmeligheden, sigtes til at skabe klar hjemmel for at fravige udgangspunktet i grundlovens § 72 om retskendelse.

Krypteret pakkedata, f.eks. en krypteret e-mail med digital signatur, indgår ikke i GovCERT's datagrundlag i ukrypteret form. Ved at kryptere meddelelser er det således muligt at forhindre, at GovCERT's personale undtagelsesvis bliver nødt til at behandle indholdet af e-mails.

Opbevaringsperioden for indsamlede oplysninger om de tilsluttede myndigheders ind- og udgående internettrafik vil maksimalt være tre år, for så vidt angår pakke- og trafikdata, der knytter sig til en konkret sikkerhedshændelse på internettet. Opbevaringsperioden påregnes dog i de fleste tilfælde at være væsentligt kortere.

Såfremt der ikke foreligger en konkret sikkerhedshændelse er de maksimale opbevaringstider væsentligt kortere, henholdsvis 14 kalenderdage for pakkedata og 12 måneder for trafikdata.

Det vurderes, at de foreslåede maksimale opbevaringsperioder er de kortest mulige i forhold til formålet med GovCERT. Det er i den forbindelse væsentligt at være opmærksom på, at GovCERT med vedtagelsen af lovforslaget alene får hjemmel til at analysere pakkedata ved begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse. Adgangen til pakkedata er yderligere begrænset af, at kun den del af de indsamlede pakkedata, som er relevant for den pågældende analyse af sikkerhedshændelsen, vil kunne analyseres. Adgangen for GovCERT til pakkedata er herved begrænset mest muligt for at imødekomme hensynet til privatlivets fred.

Den behandling af personoplysninger, som hjemlen for GovCERT til at indsamle, registrere og opbevare oplysninger om de tilsluttede myndigheders ind- og udgående internettrafik (pakke- og trafikdata) uundgåeligt vil afstedkomme, vil til enhver tid skulle overholde reglerne i persondatalovens §§ 5-8 om regler for behandling af personoplysninger.

I bestemmelsens stk. 3 foreslås den nærmere tekniske udmøntning at skulle ske administrativt. Ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler herom.

Til § 4

I bestemmelsens stk. 1 foreslås det, at persondatalovens § 35 om retten til at gøre indsigelse ikke skal finde anvendelse i forbindelse med GovCERT's aktiviteter. Bestemmelsen vil medføre, at registrerede ikke vil kunne gøre indsigelse mod GovCERT's behandling af personoplysninger.

Det vurderes således, at behovet for at gøre indsigelse i denne situation, hvor indsamlingen af personoplysninger er en nødvendig konsekvens af GovCERT's virke, er mindre fremtrædende end de administrative byrder, det vil kunne pålægge GovCERT, hvis registrerede kunne gøre indsigelse.

Der henvises i den forbindelse til afsnit 3.5.4 i de almindelige bemærkninger, og det dér anførte om persondatalovens § 35.

Bestemmelsen i stk. 2 indebærer, at GovCERT's personale er underlagt en (særlig) tavshedspligt i forhold til de nævnte oplysninger. De oplysninger, som GovCERT behandler, kan derfor ikke videregives til uvedkommende.

De personer, som GovCERT indsamler oplysninger om, har som følge af bestemmelsen heller ikke ret til indsigt i oplysningerne efter persondataloven, jf. persondatalovens § 32, stk. 2.

Bestemmelsen udelukker ikke en berettiget videregivelse af oplysninger efter lovforslagets § 5.

Til § 5

Det følger af den foreslåede bestemmelse i § 5, nr. 1, at den statslige varslingstjeneste kan videregive pakkedata og trafikdata, der knytter sig til en konkret sikkerhedshændelse, til politiet. Formålet hermed er at sikre, at politiet kan modtage oplysninger til brug for efterforskning og forfølgelse af strafbare forhold, der kan være begået i forbindelse med en konkret sikkerhedshændelse, som f.eks. et virusangreb.

Med forslaget til § 5, nr. 2, skabes hjemmel til, at den statslige varslings-tjeneste kan videregive trafikdata til danske myndigheder – det kan f.eks. være DK-CERT, som overvåger forskningsnettet – og tilsluttede private virksomheder beskæftiget med kritisk infrastruktur, hvor dette er nødvendigt som led i varslingstjenestens aktiviteter og i

henhold til varslingstjenestens formål. Det kan f.eks. være information om en konkret ip-adresse, som har angrebet en myndighed til forebyggelse af yderligere angreb.

Nr. 2 sikrer herudover, at GovCERT kan udveksle trafikdata, herunder ip-adresser, med tilsvarende varslingstjenester i andre lande i forbindelse konkrete sikkerhedshændelser på internettet.

Der vil ikke efter bestemmelsen i § 5, nr. 2, kunne videregives pakkedata, herunder eksempelvis indholdet af en e-mailkorrespondance.

Det forudsættes med bestemmelsen i § 5, at andre regler i lovgivningen om indsamling og videregivelse af oplysninger mellem forvaltningsmyndigheder ikke vil kunne anvendes i forhold til data, der er indsamlet af den statslige varslingstjeneste som led i varslingstjenestens aktivitet.

Heri ligger bl.a., at hvis politiet til brug for f.eks. efterforskning af et strafbart forhold, der ikke er begået i forbindelse med en konkret sikkerhedshændelse (jf. § 5, nr. 1), ønsker pakkedata eller trafikdata fra den statslige varslingstjeneste, må politiet gå frem efter de almindelige straffeprocessuelle regler i retsplejelovens fjerde bog og i den forbindelse efter omstændighederne indhente retskendelse.

Til § 6

Formålet med § 6 er at pålægge ministeren for videnskab, teknologi og udvikling at nedsætte et uafhængigt tilsyn, der skal følge GovCERT's virksomhed. Ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler for tilsynets virksomhed.

Det er hensigten, at tilsynet skal forestås af en dommer som formand og fire sagkyndige medlemmer, der må betragtes som upolitiske, og som beskikkes som følge af den almindelige tillid og agtelse, der er knyttet til deres person – i lighed med ordningen, der er kendt fra Wamberg-udvalget, der fører tilsyn med Politiets Efterretningstjenestes og Forsvarets Efterretningstjenestes behandling af personoplysninger. Det er en endvidere en forudsætning, at tilsynets medlemmer kan sikkerhedsgodkendes.

Datatilsynet har samtidig hermed fuld inspektionskompetence i forhold til de registrerede og opbevarede oplysninger, jf. persondatalovens § 62, stk. 2, om behandling, der

foretages for den offentlige forvaltning, og at bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige sektor, finder anvendelse.

Til § 7

En beslutning om, at en kompetence overlades generelt f.eks. af en minister til en styrelse, bør af hensyn til borgernes mulighed for at kunne vide, hvem der er rette myndighed, altid angives i en bekendtgørelse, jf. pkt. 4 i Justitsministeriets vejledning nr. 153 af 22. september 1987 om udarbejdelse af administrative forskrifter. Det foreslås derfor, at der i loven indsættes en hjemmel for ministeren for videnskab, teknologi og udvikling til at bemyndige en under Ministeriet for Videnskab, Teknologi og Udvikling oprettet styrelse eller tilsvarende institution til at udøve de beføjelser, der i loven er tillagt ministeren.

Ministeren kan herefter i en bekendtgørelse udnytte adgangen til at delegere opgaver og beføjelser til en statslig myndighed under ministeriet. Bemyndigelseshjemlen er formuleret, så den med sikkerhed kan rumme statslige myndigheder under Ministeriet for Videnskab, Teknologi og Udvikling, som organisatorisk er underordnet styrelserne. Ministeren kan således efter den foreslåede bestemmelse delegere sine beføjelser efter loven til enhver myndighed inden for ministeriets administrative hierarki uanset myndighedens placering i det administrative hierarki, herunder myndigheder, som er underordnet styrelser.

Endvidere foreslås det, at ministeren for videnskab, teknologi og udvikling efter forhandling med vedkommende minister kan bemyndige andre statslige myndigheder til at udøve de beføjelser, som i loven er tillagt ministeren for videnskab, teknologi og udvikling. Der er alene tale om statslige myndigheder. Der kan således ikke i medfør af denne bestemmelse ske delegation til private virksomheder eller organisationer. Omfanget af delegationen til den pågældende statslige myndighed skal ske efter forhandling med vedkommende minister.

Til stk. 2. Forslaget er en konsekvens af det foreslåede stk. 1. Det foreslås derfor, at ministeren for videnskab, teknologi og udvikling får hjemmel til at fastsætte regler om adgangen til at påklage afgørelser, der er truffet i henhold til bemyndigelse efter stk. 1,

herunder at afgørelserne ikke skal kunne påklages, hvilket betyder, at ministeren vil kunne afskære klageadgangen fra organisatorisk underordnede statslige myndigheder til styrelserne eller for andre statslige myndigheder. Ministeren kan f.eks. således ikke blot afskære klageadgang til ministeren, men også klageadgang til styrelserne. Adgangen til at afskære klage knytter sig kun til afgørelser på områder, som er delegeret fra ministeren i henhold til loven. Lovforslaget berører ikke øvrige klagemuligheder.

Til stk. 3. Det foreslås, at ministeren for videnskab, teknologi og udvikling får hjemmel til at fastsætte regler om udøvelsen af de beføjelser, som en anden statslig myndighed efter forhandling med vedkommende minister bliver bemyndiget til at udøve efter stk. 1. Bestemmelsen omhandler de tilfælde, hvor ministeren udnytter sin adgang til at delegere beføjelser til andre statslige myndigheder uden for Ministeriet for Videnskab, Teknologi og Udvikling.

Til § 8

Det foreslås, at loven træder i kraft den 1. juli 2011.

Til § 9

Den foreslåede bestemmelse angår lovens territoriale gyldighed. Det er hensigten med bestemmelsen at fastlægge, at GovCERT's aktiviteter ikke vedrører de grønlandske og færøske dele af riget.